

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-261423

(P2000-261423A)

(43) 公開日 平成12年9月22日 (2000.9.22)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
H 0 4 L 9/06		H 0 4 L 9/00	6 1 1 Z 5 J 1 0 4
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 A

審査請求 未請求 請求項の数 5 O L (全 11 頁)

(21) 出願番号 特願平11-58210

(22) 出願日 平成11年3月5日 (1999.3.5)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 柳澤 玲互

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100097445

弁理士 岩橋 文雄 (外2名)

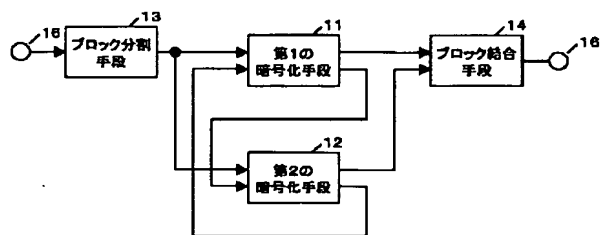
Fターム (参考) 5J104 AA18 JA03

(54) 【発明の名称】 暗号化装置

(57) 【要約】

【課題】 大規模なメモリを使用することなく、暗号化の処理速度を約2倍に改善する。

【解決手段】 ブロック分割手段13は、入力パケットをブロックに分割し、交互に第1の暗号化手段11と第2の暗号化手段12へ出力する。第1の暗号化手段11は、第2の中間データを用いてブロック暗号化を行い、第1の中間データと暗号化された第1のブロックを出力する。第2の暗号化手段12は、第1の暗号化手段11が第1の中間データを処理する遅延だけ遅れて処理を開始し、第1の中間データを用いてブロック暗号化を行い、第2の中間データと暗号化された第2のブロックを出力する。ブロック結合手段14は、暗号化された第1のブロックと第2のブロックとを結合し、暗号化されたパケットを出力する。



【特許請求の範囲】

【請求項1】 入力データを第1のブロックと第2のブロックとに分割して出力するブロック分割手段と、前記第1のブロックと第2の中間データを用い前記第1のブロックを暗号化し、第1の暗号化データと第1の中間データを出力する第1の暗号化手段と、前記第2のブロックと前記第1の中間データを用い前記第2のブロックを暗号化し、第2の暗号化データと前記第2の中間データを出力する第2の暗号化手段と、前記第1の暗号化データと前記第2の暗号化データを結合し、前記入力データを暗号化した暗号化データを出力するブロック結合手段とを備えたことを特徴とする暗号化装置。

【請求項2】 第1の暗号化手段は、第1のブロックを暗号化し第1の中間データを出力する第3の暗号化手段と、前記第1の中間データを暗号化し前記第1の暗号化データを出力する第4の暗号化手段とからなり、第2の暗号化手段は、第2のブロックを暗号化し第2の中間データを出力する第5の暗号化手段と、前記第2の中間データを暗号化し前記第2の暗号化データを出力する第6の暗号化手段とからなることを特徴とする請求項1記載の暗号化装置。

【請求項3】 ブロック分割手段は、入力データを $(m+n)$ 個 $(m, n$ は自然数)のサブブロックに分割し、分割された先頭から奇数番目の m 個の前記サブブロックを第1のブロックとして出力し、先頭から偶数番目の n 個の前記サブブロックを第2のブロックとして出力し、第1の暗号化手段は、前記第1のブロックを前記 m 個のサブブロック毎にブロック暗号化し、第2の暗号化手段は、前記第2のブロックを前記 n 個のサブブロック毎にブロック暗号化することを特徴とする請求項1または2記載の暗号化装置。

【請求項4】 第1の暗号化手段は、第2の暗号化手段が出力する j 番目 $(j=1, 2, 3, \dots, n)$ の第2の中間データを用い第1のブロックの i 番目 $(i=1, 2, 3, \dots, m)$ のサブブロックのブロック暗号化を行い、 i 番目の第1の中間データと i 番目の第1の暗号化データを出力し、

第2の暗号化手段は、前記 i 番目の第1の中間データを用い第2のブロックの j 番目の前記サブブロックのブロック暗号化を行い、前記 j 番目の第2の中間データと j 番目の第2の暗号化データを出力することを特徴とする請求項3記載の暗号化装置。

【請求項5】 第1の暗号化手段は、 i 番目の第1の中間データを遅延 T で、 i 番目の第1の暗号化データを前記遅延 T の2倍の遅延で出力し、第2の暗号化手段は、 j 番目の第2の中間データを前記遅延 T で、 j 番目の第2の暗号化データを前記遅延 T の2倍の遅延で出力し、かつ前記第1の暗号化手段より前記遅延 T だけ遅れて暗号化を行うことを特徴とする請求

項4記載の暗号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルビデオレコーダー、セット・トップ・ボックス(Set Top Box)、パーソナルコンピュータ等で、不正コピーを防止する際のコンテンツの暗号化等に用いられる、暗号化装置に関するものである。

【0002】

【従来の技術】従来、暗号化装置として、特開平9-230788号公報に記載されたものが知られている。

【0003】図6に、従来の暗号化装置のブロック図を示す。図6において、61は第7の暗号化手段、62は第8の暗号化手段、63は第9の暗号化手段、641~646は暗号化回路、65はレジスタ、66は排他的論理和演算子、67は暗号鍵、68は平文入力端子、69は暗号文出力端子である。以下、図6を用いて、従来の暗号化装置について説明する。

【0004】暗号化回路641~646は、暗号化されていないデータ(以下、平文と呼ぶ)を暗号鍵67に基づいて暗号化し、暗号化されたデータ(以下、暗号文と呼ぶ)を出力する。一般に、暗号の強度を増すため、暗号化回路は同じ構成のものが多数直列に接続される。図6では、 $X1$ から Xma (ma は自然数)までの ma 個の同じ構成の暗号化回路と、 $Y1$ から Ymb (mb は自然数)までの mb 個の同じ構成の暗号化回路とを直列に接続している。図6ではこれらのうち $X1$ (暗号化回路641)、 $X2$ (暗号化回路642)、 Xma (暗号化回路643)、 $Y1$ (暗号化回路644)、 $Y2$ (暗号化回路645)、 Ymb (暗号化回路646)の6個を例として示した。このように暗号化回路を多数接続して強度を増す例としては、米国における標準方式であるDES(Data Encryption Standard)が知られている。

【0005】端子68からは、例えば64ビットの平文が入力され、暗号化回路641~646でブロック暗号化が行われる。例えば、MPEG2(Moving Picture Experts Group 2)のTSP(Transport Stream Packet)(以下、単にTSPと呼ぶ)を暗号化する場合、TSPは8ビット長であるので、図示していない変換回路にて8個のTSPをひとまとめにして64ビット長の平文に変換した後、端子68から入力する。

【0006】図6では、暗号化回路641~643で構成される第8の暗号化手段62の出力を、一旦レジスタ65に記憶し、次の平文が入力された時に、演算子66でレジスタ65と次の平文との排他的論理和をとる構成にしている。これはCBC(Cipher Block Chaining)モードと呼ばれ、暗号文の解読を困難にするための一つの手法である。

【0007】例えばTSPの場合、先頭から64ビット毎にサブブロックに分割し、端子68より入力する。こ

のサブブロックを先頭から順に第1サブブロック、第2サブブロック、第3サブブロックと呼ぶことにすると、まず第8の暗号化手段62で第1サブブロックのブロック暗号化を行い、結果を第9の暗号化手段63に出力するとともにレジスタ65に蓄える。暗号化回路644～646で構成される第9の暗号化手段63は、引き続き第1サブブロックのブロック暗号化を行い、暗号化された第1サブブロックを端子69より出力する。

【0008】次に、端子68より入力された第2サブブロックは、レジスタ65と演算子66で排他的論理和がとられた後、暗号化回路641～643でブロック暗号化が行われる。この結果はレジスタ65に蓄えられ、次の第3サブブロックのブロック暗号化に使用される。また、第9の暗号化手段63では引き続きブロック暗号化を行い、暗号化された第2サブブロックを端子69より出力する。

【0009】上記した処理をTSPの終わりまで繰り返し行うことで、1パケット分の暗号化を行うことができる。なお、端子69からはサブブロックに分割された暗号文が出力されるため、図示していない逆変換回路にて、サブブロックをTSPに逆変換することで、暗号化されたTSPが得られる。

【0010】CBCモードとしては、図7のような構成も知られている。図7では、レジスタ65と暗号鍵67との排他的論理和をとった結果を、次の平文の暗号鍵としている。図6、図7のいずれにせよ、第8の暗号化手段62の出力と入力された平文から、次の暗号化を行い、結果を第9の暗号化手段でさらに暗号化することで、端子69より暗号文が出力される。

【0011】図6あるいは図7の動作を、タイミングチャートにして図8に示す。入力される平文P10、P20に対して、第7の暗号化手段61の処理遅延T0だけ遅れて、暗号文C10、C20が出力される。TSPの場合、1パケットが188バイトであるから、24のサブブロックに分割される。よって、1パケット分の処理遅延TXは $TX = 24 \times T0$ となる。

【0012】第7の暗号化手段61の処理遅延T0は、暗号化回路641～646各々の処理遅延と、全体の段数($ma + mb$)で決定される。これらは共に暗号の強度に関係し、暗号の強度をある一定レベル以上に保つためには、処理遅延T0をある遅延より小さくすることができない。すなわち、1パケット分の処理遅延TXをある遅延より短くすることができない。よって、高いビットレートのTSPに対しては、第7の暗号化手段61を複数用意し、それらを並列に処理することで、見かけ上の処理遅延を短くする必要がある。

【0013】図9に、約2倍のビットレートのTSPまで、処理を行う場合の構成を示す。図9において、91は第10の暗号化手段、92～95はバッファ、96はパケット分割手段、97はパケット結合手段である。以

下、図9を用いて、約2倍のビットレートのTSPを、暗号化する場合を説明する。

【0014】第10の暗号化手段91は、図10に示すように第7の暗号化手段61と全く同じ構成を有し、第11の暗号化手段92と第12の暗号化手段93によるCBCモードを備え、1パケットのブロック暗号化を行う。なお、第7の暗号化手段61が図7のCBCモードを備えるときは、同様に図11のCBCモードを備えている。

【0015】端子68より入力されるTSPは、1パケット毎にパケット分割手段96で分割され、1パケット毎にバッファ92およびバッファ93へ、交互に書き込まれる。ここで、バッファ92、バッファ93は、例えばFIFO(First In First Out memory)である。

【0016】バッファ92に書き込まれたTSPは、第7の暗号化手段61で暗号化され、バッファ94に書き込まれる。同様にバッファ93に書き込まれたTSPは、第10の暗号化手段91で暗号化され、バッファ95に書き込まれる。ここで、バッファ94、バッファ95は、例えばFIFOである。

【0017】この時のタイミングチャートを、図12に示す。以下、図12を用いて、図9の動作を説明する。

【0018】端子68から入力されたTSPであるP100、P200、P300、P400は、パケット分割手段96で分割され、P100、P300はバッファ92に、P200、P400はバッファ93に書き込まれる。第7の暗号化手段61はP100、P300を順次暗号化し、結果の暗号文C100、C300をバッファ94に書き込む。同様に、第10の暗号化手段91はP200、P400を順次暗号化し、結果の暗号文C200、C400をバッファ95に書き込む。

【0019】パケット結合手段97は、バッファ94、バッファ95より交互に暗号文を読み出す。これにより、端子68から入力されるP100、P200、P300、P400を暗号化した結果C100、C200、C300、C400が端子69より順次出力される。また、この時、第7の暗号化手段61と第10の暗号化手段91とが並列に動作するため、図8に比べて約2倍のビットレートのTSPまで、図12では処理している。

【0020】

【発明が解決しようとする課題】しかしながら上記した従来の構成では、約2倍のビットレートのTSPを処理するために、新たにFIFOを追加する必要があり、回路規模の増大とコストの上昇を招くという問題点を有していた。

【0021】本発明は上記従来の問題点を解決するもので、FIFOを追加しなくとも約2倍のビットレートのTSPまで処理可能な、暗号化装置を提供することを目的とする。

【0022】

【課題を解決するための手段】この課題を解決するために本発明は、入力データを第1のブロックと第2のブロックとに分割して出力するブロック分割手段と、前記第1のブロックと第2の中間データを用い前記第1のブロックを暗号化し、第1の暗号化データと第1の中間データを出力する第1の暗号化手段と、前記第2のブロックと前記第1の中間データを用い前記第2のブロックを暗号化し、第2の暗号化データと前記第2の中間データを出力する第2の暗号化手段と、前記第1の暗号化データと前記第2の暗号化データを結合し前記入力データを暗号化した暗号化データを出力するブロック結合手段とから構成されている。

【0023】

【発明の実施の形態】本発明は、ブロック分割手段で、入力データを第1のブロックと第2のブロックとに分割する。第1の暗号化手段は、第2の中間データを用い、第1のブロックを暗号化し、第1の中間データと第1のブロックを暗号化した結果である第1の暗号化データを出力する。第2の暗号化手段は、第1の中間データを用い、第2のブロックを暗号化し、第2の中間データと第2のブロックを暗号化した結果である第2の暗号化データを出力する。ブロック結合手段は、第1の暗号化データと第2の暗号化データを結合し、入力データを暗号化した暗号化データを出力する。

【0024】以下、本発明の実施の形態について、図面を用いて説明する。

【0025】（実施の形態1）図1は、本発明の実施の形態1による暗号化装置のブロック図を示すものである。図1において、11は第1の暗号化手段、12は第2の暗号化手段、13はブロック分割手段、14はブロック結合手段、15は平文入力端子、16は暗号文出力端子である。以下、図1を参照しながら、本実施の形態の暗号化装置について説明する。

【0026】ブロック分割手段13は、端子15より入力される平文を、2つのブロックに分割する。例えば端子15よりTSPが入力される場合、まず先頭から64ビット毎のサブブロックに分割し、次に先頭から1番目、3番目、5番目、・・・、すなわち、奇数番目のサブブロックを第1のブロックとして、第1の暗号化手段11に出力する。同様に先頭から偶数番目のサブブロックを、第2のブロックとして、第2の暗号化手段12に出力する。このような動作を行うブロック分割手段13には、例えばデマルチプレクサが用いられる。

【0027】第1の暗号化手段11と第2の暗号化手段12の構成例を、図2に示す。図2において、21は第3の暗号化手段、22は第4の暗号化手段、23は第5の暗号化手段、24は第6の暗号化手段、251～256および261～266は暗号化回路、27、28はレジスタ、29、210は排他的論理和演算子、211、212は暗号鍵である。以下、図2を参照しながら、第

1の暗号化手段11と第2の暗号化手段12の暗号化の動作について説明する。

【0028】第1の暗号化手段11は、第1のブロックの暗号化を、暗号鍵211を用いて行う。まず1番目のサブブロックが入力されると、暗号化回路251～253でブロック暗号化を行い、1番目の第1の中間データを出力する。従来の技術の項で説明したように、暗号の強度を増すため、同様の構成の暗号化回路251～253を ma 段直列に接続している。

【0029】第1の暗号化手段11、第2の暗号化手段12は、共にCBCモードを有しており、入力されるサブブロックとレジスタ27、28との排他的論理和を演算子29、210で行う構成をとっている。CBCモードとしては、図3に示すように、レジスタ27、28と暗号鍵211、212との排他的論理和をとる構成としてもよい。

【0030】1番目の第1の中間データは、引き続き暗号化回路254～256でブロック暗号化され、暗号化された1番目のサブブロックとして出力されるとともに、第2の暗号化手段12のレジスタ28に一旦蓄えられる。暗号化回路254～256は mb 段で構成され、暗号化回路251～253と合わせて、全体で $ma+mb=m$ 段（ m は自然数）の暗号化回路を構成している。

【0031】第2のブロックの暗号化は第2の暗号化手段12で行われるため、2番目のサブブロックが入力されると、まずレジスタ28に蓄えられている1番目の第1の中間データと、2番目のサブブロックとの排他的論理和が、演算子210でとられる。次に、 na 段（ na は自然数）の暗号化回路261～263で、暗号鍵212を用いたブロック暗号化が行われ、1番目の第2の中間データが出力される。

【0032】1番目の第2の中間データは、引き続き nb 段（ nb は自然数）の暗号化回路264～266でブロック暗号化され、暗号化された2番目のサブブロックとして出力されるとともに、第1の暗号化手段11のレジスタ27に一旦蓄えられる。暗号化回路254～256と、暗号化回路251～253とを合わせて、全体で $na+nb=n$ 段（ n は自然数）の暗号化回路を構成している。

【0033】次に3番目のサブブロックが入力されると、レジスタ27に蓄えられた1番目の第2の中間データとの排他的論理和が演算子29でとられ、暗号化回路251～253でブロック暗号化され、2番目の第1の中間データが出力される。これを一旦レジスタ28に蓄えるとともに、暗号化回路254～256でブロック暗号化し、暗号化された3番目のサブブロックとして出力する。

【0034】同様の操作を繰り返すことで、暗号化されたサブブロックが次々に出力される。この時のタイミングチャートを図4に示す。図4では、第3の暗号化手段

の処理遅延を T_3 、第4の暗号化手段の処理遅延を T_4 、第5の暗号化手段の処理遅延を T_5 、第6の暗号化手段の処理遅延を T_6 、第1の暗号化手段の処理遅延を $T_1 (=T_3+T_4)$ 、第2の暗号化手段の処理遅延を $T_2 (=T_5+T_6)$ とし、 $T_3=T_4=T_5=T_6$ の場合を示した。なお、この時、 $m_a=m_b=n_a=n_b$ 、すなわち $m=n$ である。

【0035】第3の暗号化手段の処理遅延 T_3 後、1番目の第1の中間データが出力され、さらに第4の暗号化手段の処理遅延 T_4 の後、暗号化された1番目のサブブロックが出力される。暗号化手段12は、第3の暗号化手段の処理遅延 T_3 だけ遅れて処理を開始する。すなわち、1番目の第1の中間データが出力されてから処理を開始する。第5の暗号化手段の処理遅延 T_5 の後、1番目の第2の中間データが出力され、さらに第6の暗号化手段の処理遅延 T_6 の後、暗号化された2番目のサブブロックが出力される。

【0036】以下同様に、第1の暗号化手段11と第2の暗号化手段12とがサブブロック毎に交互に動作し、端子15より入力される平文の暗号化を行う。ブロック結合手段14は、第1の暗号化手段11と第2の暗号化手段12とが出力するサブブロック毎の暗号文を交互に出力することで、端子15より入力される平文の暗号文を、端子16より出力する。このような動作を行うブロック結合手段14には、例えばマルチプレクサが用いられる。

【0037】図5に、平文としてTSPを用いた場合のタイミングチャートを示す。図5において、 $P_1 \sim 4$ は入力されるTSP、 $C_1 \sim 4$ が暗号化されたTSPである。暗号化されたTSPである $C_1 \sim 4$ は、入力TSPである $P_1 \sim 4$ より暗号化の処理遅延だけ遅れて出力される。この処理遅延は図4、図5に示すように、 T_3+T_5 になる。

【0038】また、TSPの場合、1パケットが188バイトであるから、1パケットは24のサブブロックに分割される。よって、第1の暗号化手段11の処理遅延 T_A は $12 \times T_1$ 、第2の暗号化手段12の処理遅延 T_B は $12 \times T_2$ となる。この処理遅延 T_A 、 T_B は、 $T_1=T_2$ 、 $T_3=T_4=T_5=T_6$ の時最小となり、第1の暗号化手段11単独で暗号化した時の処理遅延 $24 \times T_1$ 、あるいは第2の暗号化手段12単独で暗号化した時の処理遅延 $24 \times T_2$ の、約2倍のビットレートのTSPまで処理することが可能になる。

【0039】なお、本実施例では、平文がTSPの場合を例にとって説明したが、どのような平文に対しても、最大で約2倍の処理速度で暗号化を行うことができる。

また、処理速度が最小となる $T_1=T_2$ 、 $T_3=T_4=T_5=T_6$ の場合を説明したが、この条件に当てはまらない場合でも、処理速度を改善することができ、ビットレートの高い平文に対して効果がある。

【0040】

【発明の効果】以上のように本発明によれば、入力データを第1のブロックと第2のブロックとに分割して出力するブロック分割手段と、第2の中間データを用い第1のブロックを暗号化し第1の暗号化データと第1の中間データを出力する第1の暗号化手段と、第1の中間データを用い第2のブロックを暗号化し第2の暗号化データと第2の中間データを出力する第2の暗号化手段と、第1の暗号化データと第2の暗号化データを結合し暗号化データを出力するブロック結合手段とを設けることにより、大容量のメモリを使用しなくとも容易に暗号化の処理速度が改善でき、その実用的効果は大きい。

【図面の簡単な説明】

【図1】本発明の実施の形態1における暗号化装置の構成を示すブロック図

【図2】同実施の形態1における第1の暗号化手段および第2の暗号化手段の具体的な構成例を示すブロック図

【図3】同実施の形態1における別のCBCモードの構成例を示すブロック図

【図4】同実施の形態1における第1の暗号化手段および第2の暗号化手段の動作を説明する信号波形図

【図5】同実施の形態1における暗号化装置の動作を説明する信号波形図

【図6】従来の暗号化装置の構成を示すブロック図

【図7】従来の暗号化装置における別のCBCモードでの構成例を示すブロック図

【図8】従来の暗号化装置の動作を説明する信号波形図

【図9】従来の暗号化装置を約2倍の処理速度で動作させる場合の構成例を示すブロック図

【図10】従来の暗号化装置における第10の暗号化手段の具体的な構成例を示すブロック図

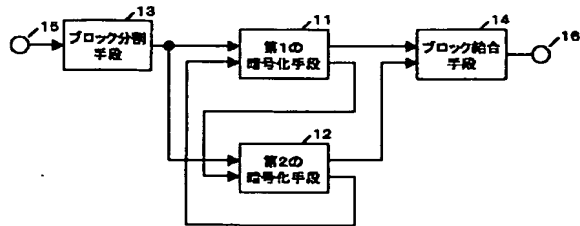
【図11】従来の暗号化装置における第10の暗号化手段の別のCBCモードでの具体的な構成例を示すブロック図

【図12】従来の暗号化装置を約2倍の処理速度で動作させる場合の動作を説明する信号波形図

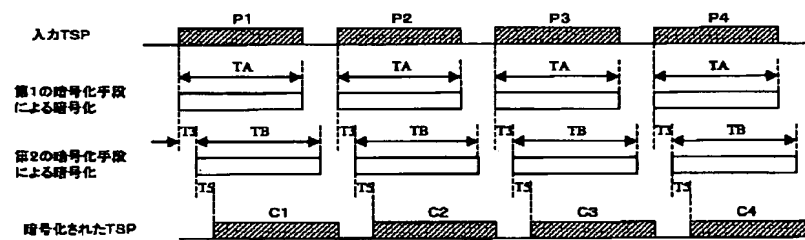
【符号の説明】

- 11 第1の暗号化手段
- 12 第2の暗号化手段
- 13 ブロック分割手段
- 14 ブロック結合手段

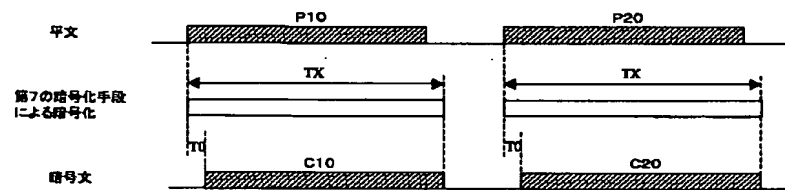
【図1】



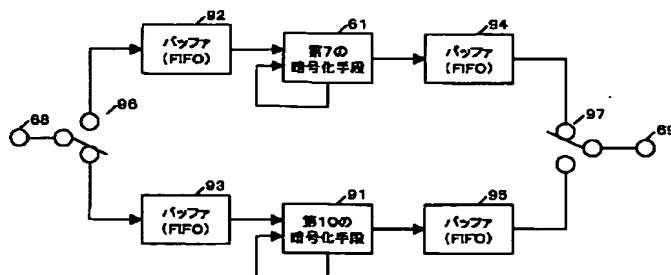
【図5】



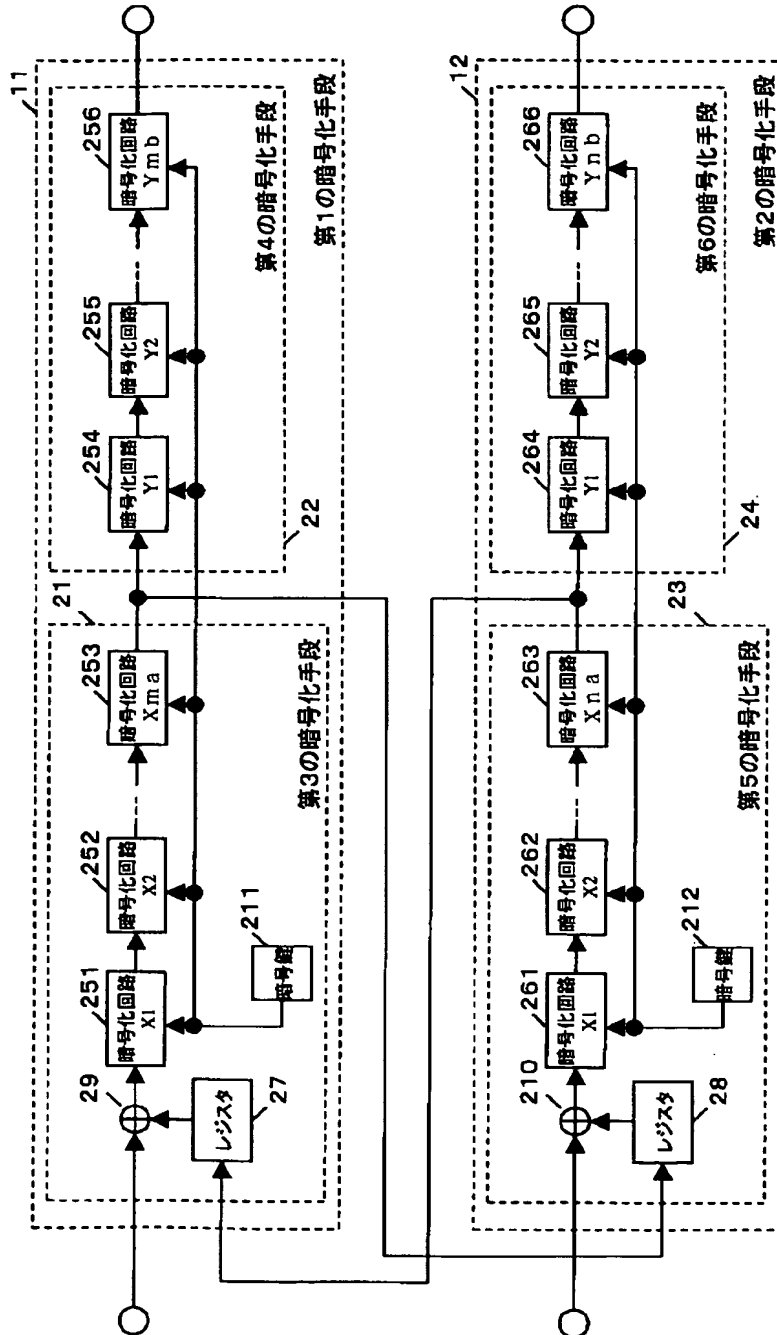
【図8】



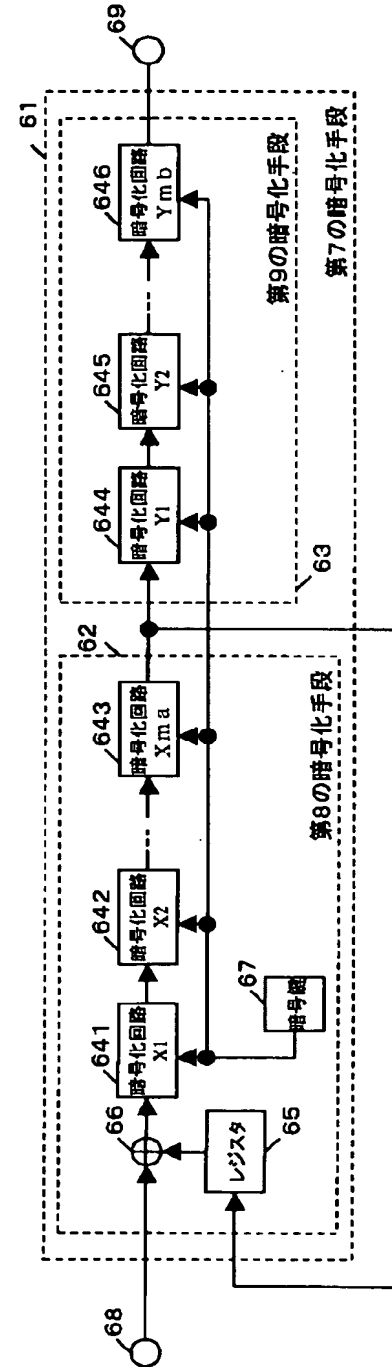
【図9】



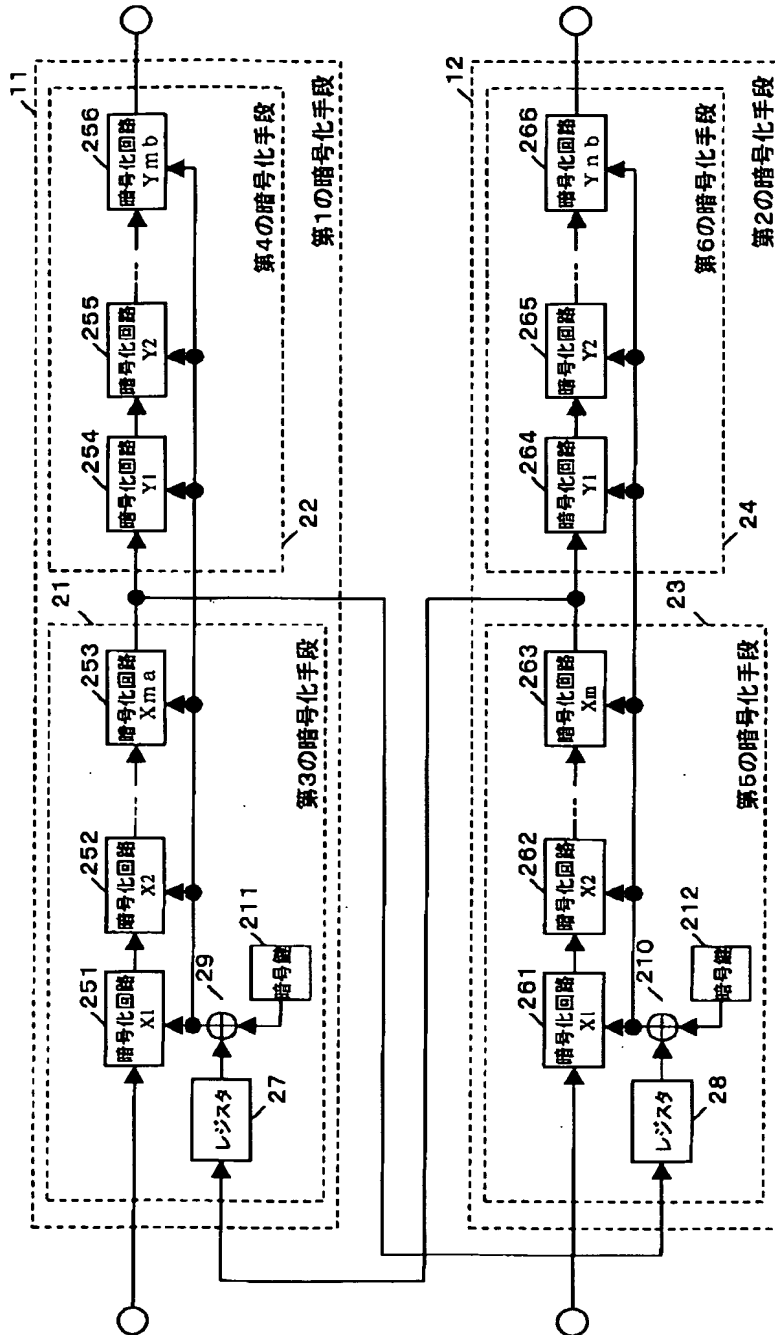
【図2】



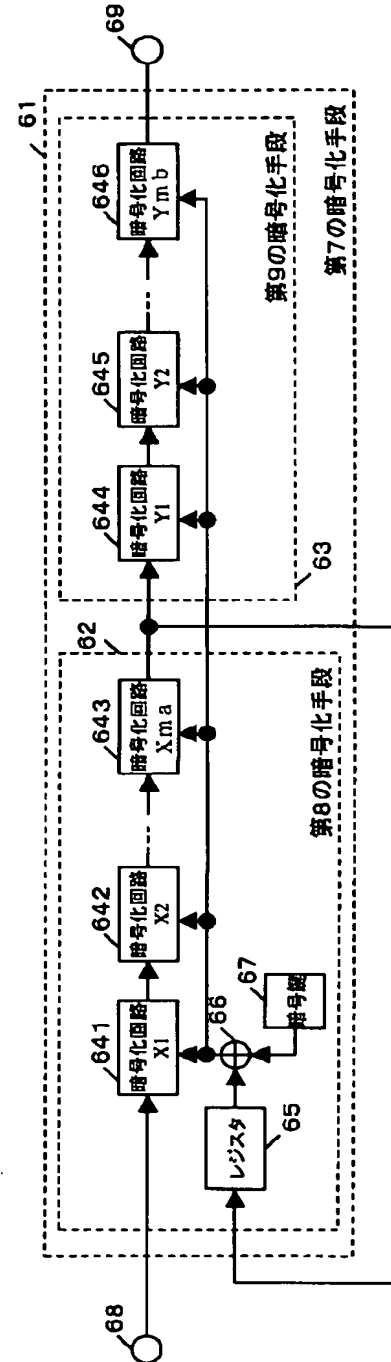
【図6】

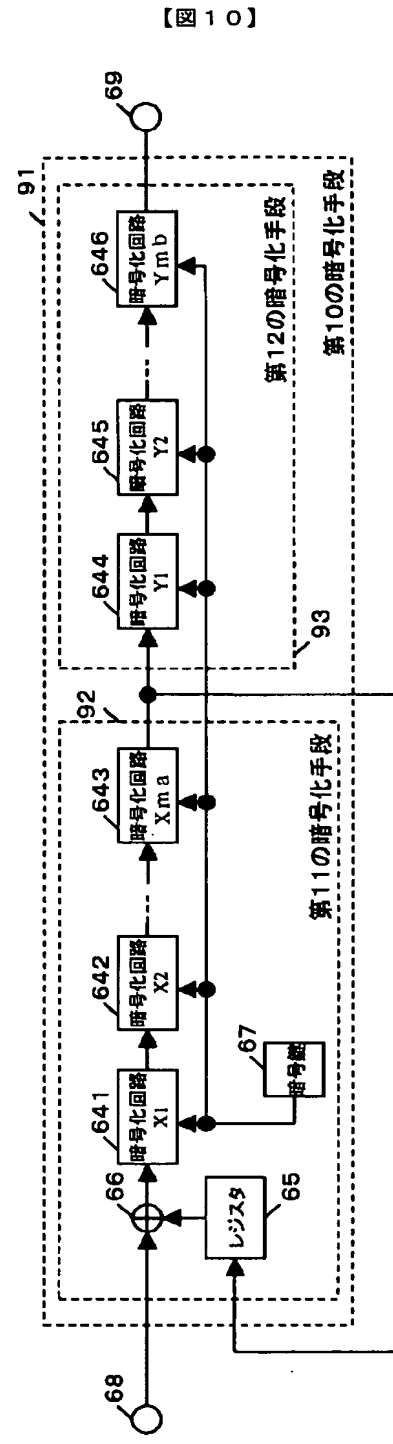
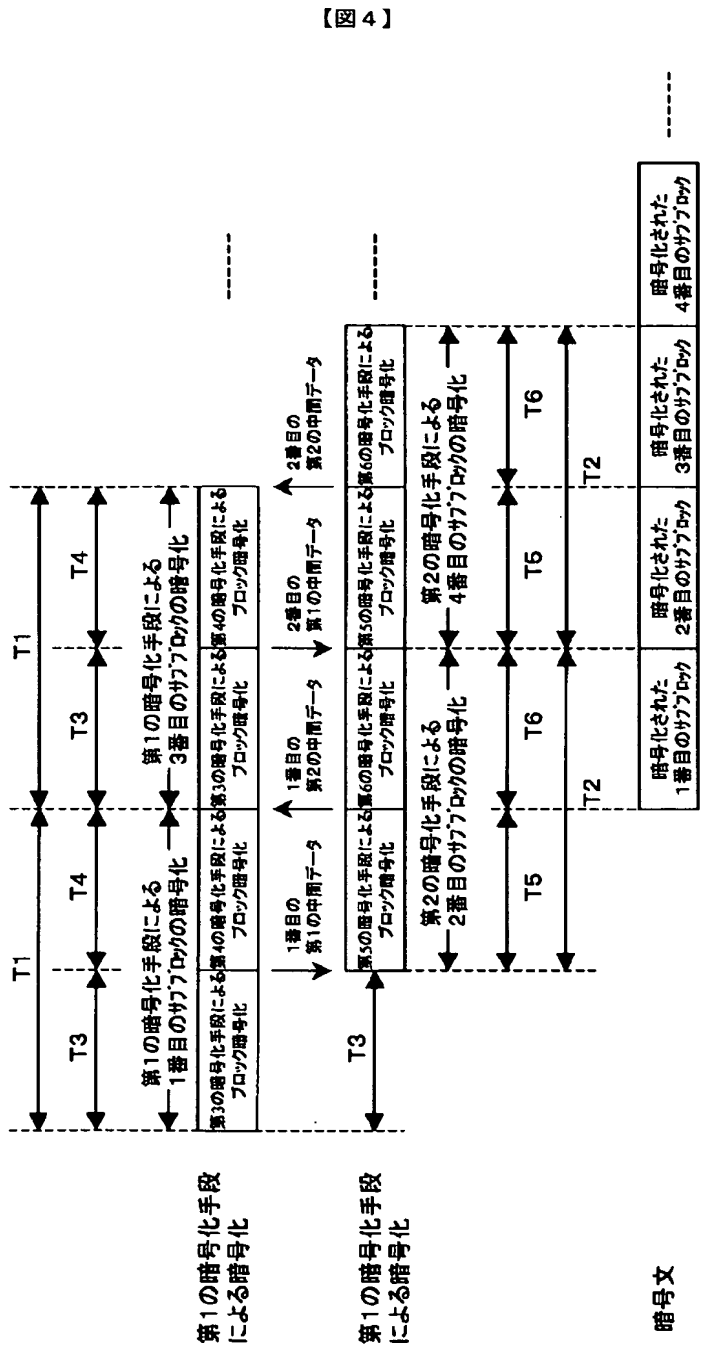


【図3】

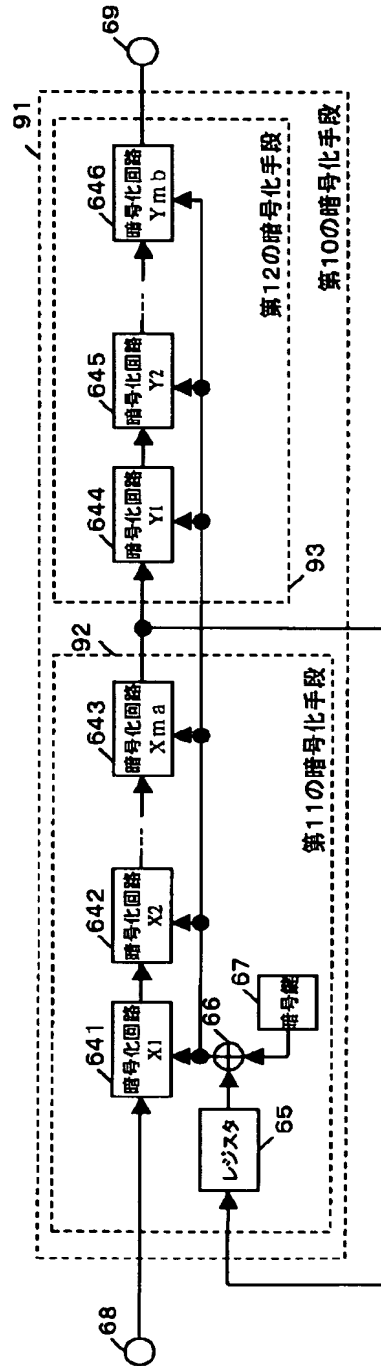


【図7】





【図11】



【図12】

